DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

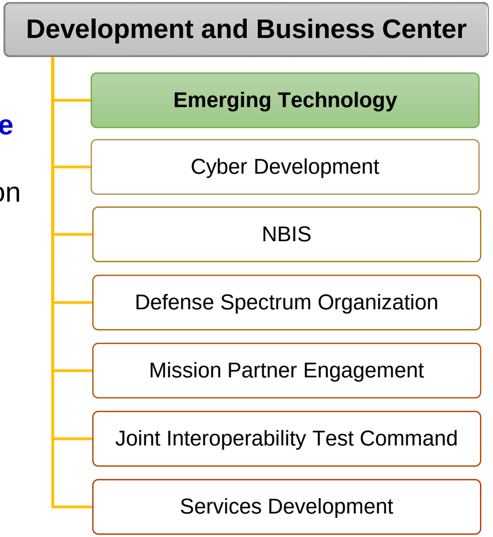
Assured Identity

Commercial Innovation to the Tactical Edge

Major Nikolaus Ziegler, USA
DISA Emerging Technology
14 May 2019

Emerging Technology Directorate EMD

Mr. Steve Wallace
301-225-9500
Systems Innovation Scientist



Development and Business Center

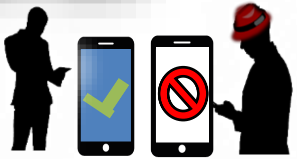
- **Emerging Technology**
- Cyber Development
- NBIS
- Defense Spectrum Organization
- Mission Partner Engagement
- Joint Interoperability Test Command
- Services Development

Mission

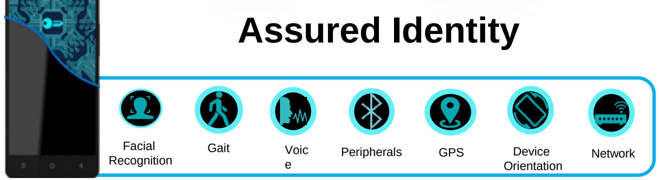
Serve as the authoritative organization to identify and deliver innovative processes, services, and capabilities across all facets of DISA's operating model. As the lead innovations integrator, collaborate with, and share lessons learned and innovative practices with mission and industry partners.

Cloud-based Internet Isolation

Mobile Hardening



Assured Identity



Continuous Multi-Factor Authentication (CMFA)

Commercial Solutions For Classified

Mobile/Desktop Convergence

CODE
PLAN
DEPLOY
OPERATE
MEASURE
RELEASE
TEST
BUILD

DevSecOps

Emerging Technology Directorate

Our Mission

Serve as the authoritative organization to identify and deliver innovative processes, services, and capabilities across all facets of DISA’s operating model. As the lead innovations integrator, collaborate with, and share lessons learned and innovative practices with mission and industry partners.

Directorate Build: 3 Divisions

Innovation Support

- Collaboration and Outreach programs among agency, mission, and industry partners
- Subject Matter Expertise in prioritized emerging technologies
- Program Support: Rapid Innovation Fund (RIF), Technical Exchanges (TEMs), Cooperative Research and Development Activities (CRADAs), etc.

Collaboration and Defense

- Support to Cyber and Services Development Directorates

Infrastructure

- Support to Infrastructure and Services Executive Directorates

Collaboration and Defense & Infrastructure work directly with technical leadership to find appropriate technologies/processes and programs to test and potentially deploy.

Emerging Technology Pillars of Action

Facilitate the Agency's ability to identify, explore, sponsor, develop, and introduce new technologies that align with the Director's priorities and possess potential for **addressing gaps** in enterprise cyber capabilities.

Rapidly assess the value of innovative technologies through **limited fielding** events and position those of merit toward operational transition.

Holistically support Agency initiatives and assist in the **streamlining of current capabilities**.

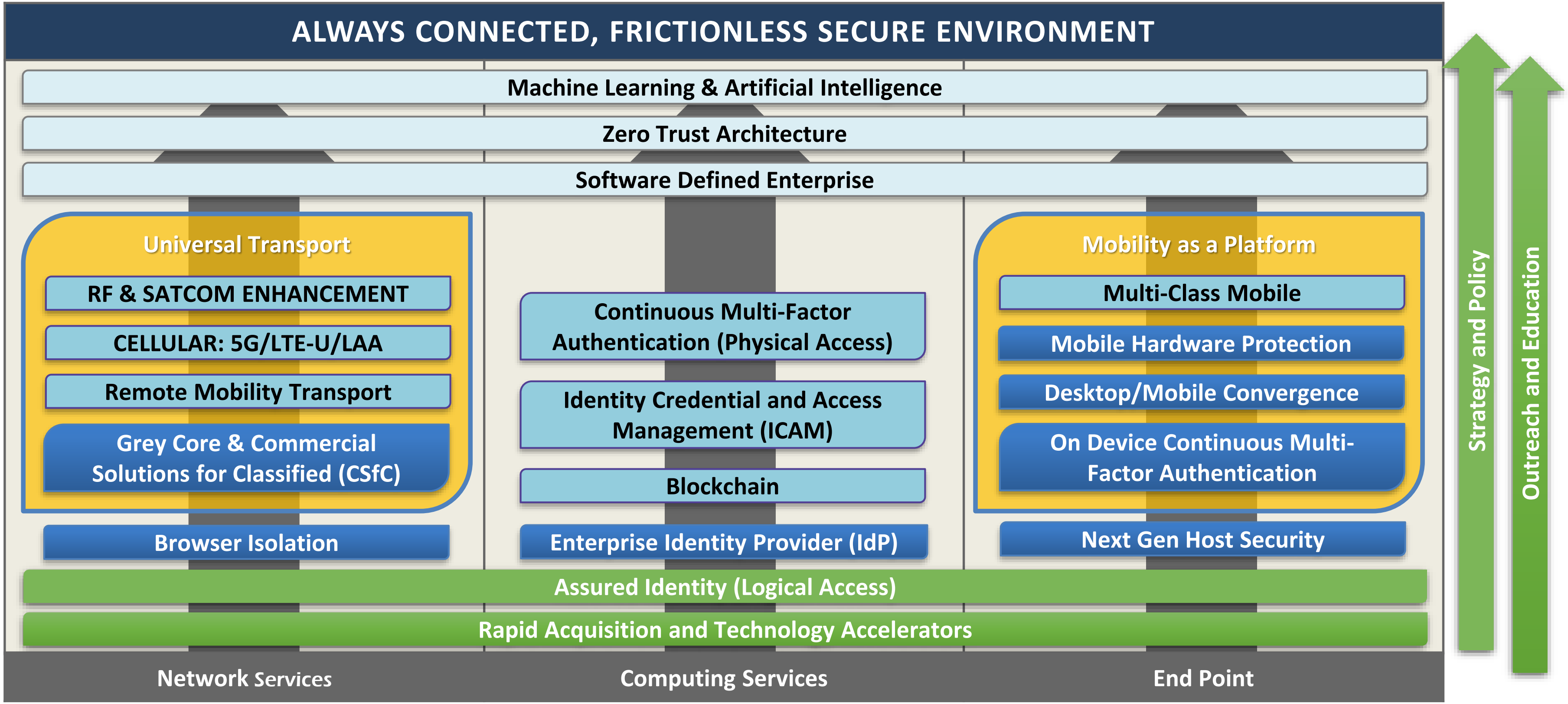
Boost **internal and external collaboration** for the innovators of DISA.

Strengthen the Agency's ability to **succeed or fail fast.**

DISA CMFA Video

DISA

EMD Technology Roadmap



ALWAYS CONNECTED, FRICTIONLESS SECURE ENVIRONMENT

Machine Learning & Artificial Intelligence

Zero Trust Architecture

Software Defined Enterprise

Universal Transport

- RF & SATCOM ENHANCEMENT
- CELLULAR: 5G/LTE-U/LAA
- Remote Mobility Transport
- Grey Core & Commercial Solutions for Classified (CSfC)

Browser Isolation

Continuous Multi-Factor Authentication (Physical Access)

Identity Credential and Access Management (ICAM)

Blockchain

Enterprise Identity Provider (IdP)

Mobility as a Platform

- Multi-Class Mobile
- Mobile Hardware Protection
- Desktop/Mobile Convergence
- On Device Continuous Multi-Factor Authentication

Next Gen Host Security

Assured Identity (Logical Access)

Rapid Acquisition and Technology Accelerators

Network Services

Computing Services

End Point

Strategy and Policy

Outreach and Education

● = Actively Engaged ● = Actively Pursuing ○ = Monitoring ● = Enabling Activities

Today's Information Environment: Cumbersome

Difficult – Time Consuming – Equipment Heavy

Authentication

- User IDs and passwords
- Two-factor
- Point-in-time
- Lockouts and resets

Ecosystem

- Multiple devices
- Reliance on net security
- Data is on premise and on device
- Transport requires hardened and dedicated networks

DISA

Mobility

Ensuring a Secure Emergency Commercial–Civilian–Military Communications Platform

Identification

Medical Records

Credit/Debit Cards

ATMs

Financial Transactions

Digital Gold Standard/Currency

FirstNet™
Emergency Comms

Type 1 Encryption	MAC	GPS Info		PIN	Biometrics	Int’l Encryption
0 1 0 0 1 1 1 0 0 1 0 1 1 0 0 1	56:75:6c:63:61:6e	40.70699	-74.01127	* * * *	A A A T G C G C C C G C	0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 1

Cyber Incidents

ebay
JPMorganChase

Bottom Line

Cyber attacks erode consumer and investor confidence and are a national security threat.

+ **ENCRYPTION**
+ **SPECTRUM**
+ **PHYSICAL SECURITY**
+ **IDENTITY MANAGEMENT**

= **Commercial/Civilian (Secure):**

Voice
Banking
DATA
Assured Identity
Apps
Police
Fire
RESCUE

Civilian/Military (Secure):

Voice
U/S/TS Capable
DATA
Assured Identity
Military Apps

Information Environment of the Future: Seamless

Always connected – more secure – better user experience

Benefits

- Frictionless environment
- Continuous multifactor authentication - dynamic
- Cost savings/avoidance

Ecosystem

- One mobile endpoint
- Multi-domain
- Virtual environments
- Defense in depth; no single points of failure

Our Focal Point – Assured Identity

The Goal: Assurance and protection of the warfighter’s identity using their mobile device.

Key Steps to Assured Identity:

Hardware Attestation

A digital key etched into mobile device hardware provides trust for sensor data and locally generated keys.

Continuous Multifactor Authentication (CMFA)

- Sensor data - behavioral and contextual biometric factors – machine–learning algorithms
- Continuous authentication in mobile, desktop, or server environments
- Enables physical and logical access without passwords

Personalized Contextual Authentication

CMFA constantly verifies identity

Facial Recognition

Gait

Voice

Peripherals

GPS

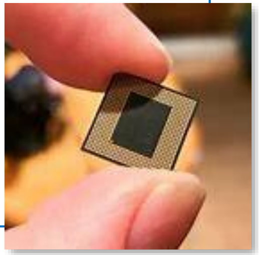
Device Orientation

Network

Android Assured Identity Solution

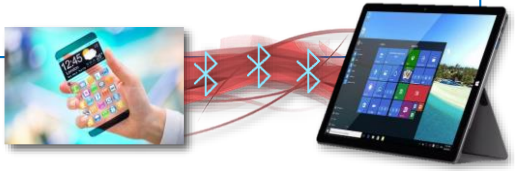
CMFA

- Fusion Algorithm
  - Biometric data from mobile sensors
  - Assigns a trust score for logical and physical device access
- Security policy defines trust score, time of authentication, and levels of access
- Developed on a Qualcomm Snapdragon 845 chipset
  - 2019 and beyond - SD855 in mainstream devices



Access

- Certificates leverage PureBred keychain for authentication.
- Secure Bluetooth connection to a Windows PC; credentials are unlocked based on trust score

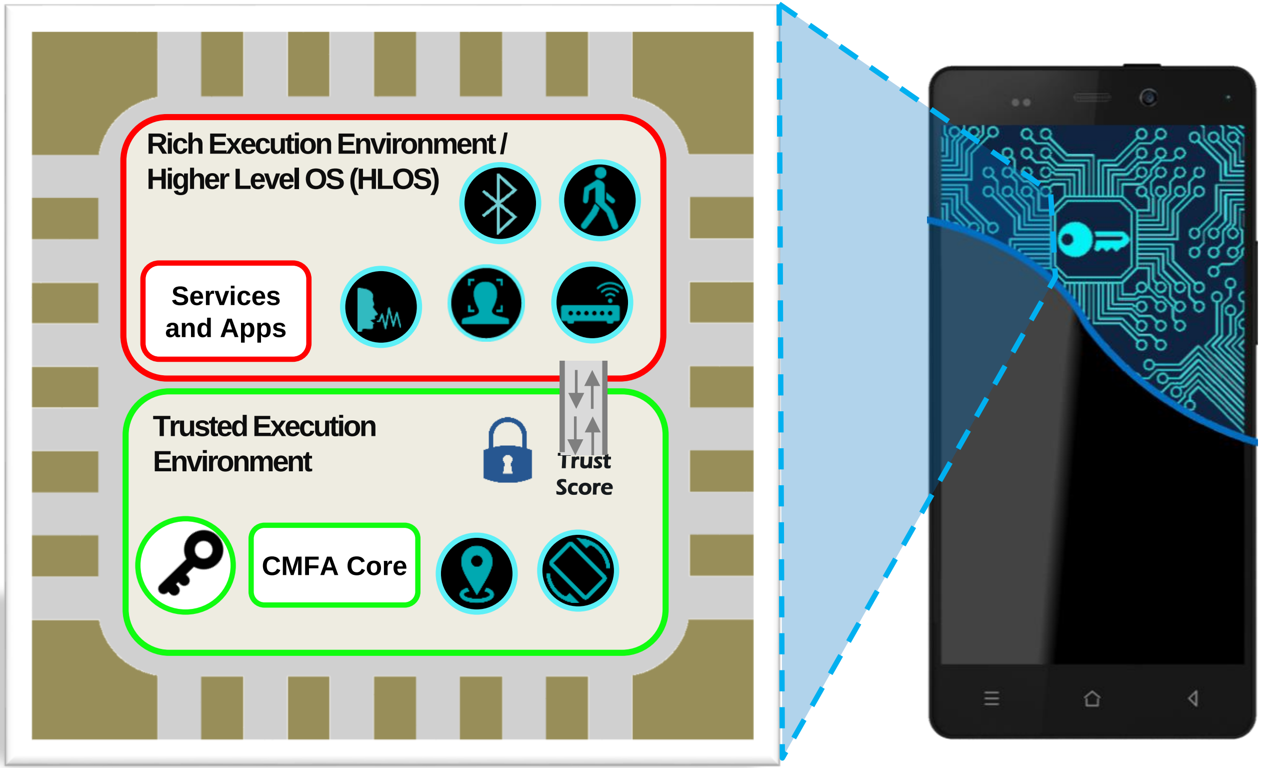


Authentication with Mobility

ARM TrustZone: TEE and REE

Increased Trust

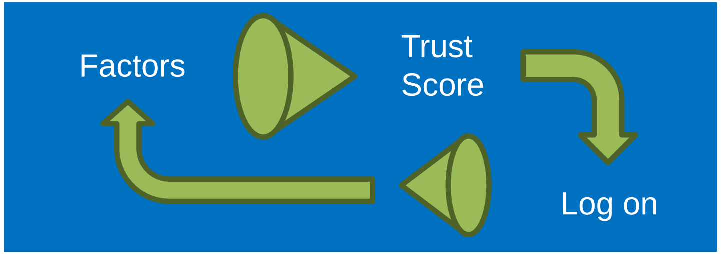
Leverage commercially designed and manufactured cryptographic objects for signing sensor data

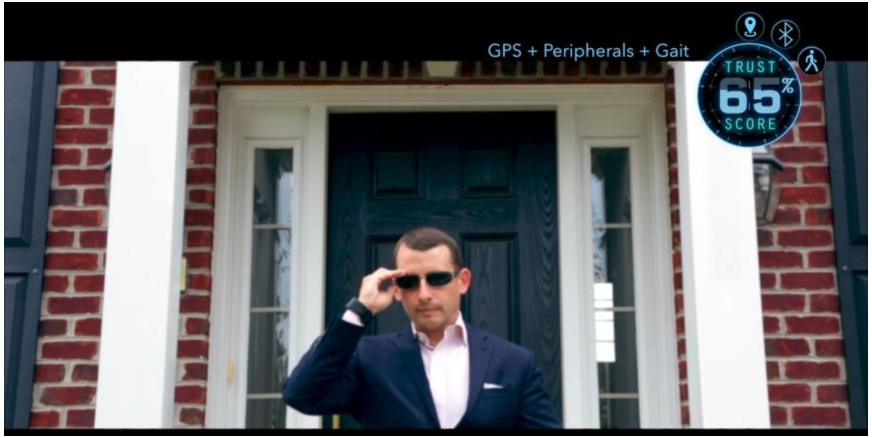

Rich Execution Environment / Higher Level OS (HLOS)
Services and Apps
Trusted Execution Environment
Trust Score
CMFA Core

Next Generation Identity and Authentication

Use Case:

- Password enhancement, computer access and potential physical access to government facilities
- Augmentation of the Public Key Infrastructure (PKI) form factor for authentication
- Improvement to “point in time” authentication





- Mobile, secure transactions with wearable technology
- Seamless access to campus areas
- Laptop authentication via mobile device (BLE, NFC)

Result: A trust score that is perpetually validated

Enhanced Samsung Knox

Samsung Knox

Customization required; allows other ID factors to unlock the Secure Workspace (CMFA)

Integration Wearables

Enhanced security and convenience in comprehensive workspace

Desktop Convergence

A secure mobile device to replace traditional laptops and desktops. Projects a desktop environment and maintains CMFA authentication

Customization of Android Secure Environment

Desktop Replacement

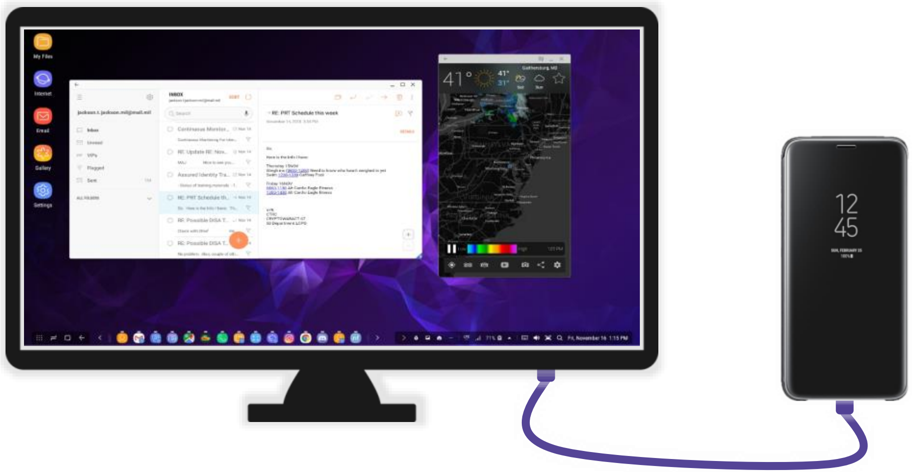
Mobile Solution to Traditional Desktop

- Samsung DeX is a desktop experience for your phone
- DeX displays a desktop-like environment to a monitor using a dock, and connected Bluetooth or wired peripherals

Phone functions as a desktop

- Email, PDF, and document editing are all fully supported, as well as many other common apps

Ability to use Samsung Knox, user certificates and credentials



Personalized Contextual Authentication

The Goal: Monitor contextual factors on the device to assure warfighter identity

Contextual Factors	Monitors user’s gait, app usage, type, swipe, interactive motion, and location
Machine Learning	• Uses deep neural networks to create a highly personalized model • This model is trained continuously and is updated regularly or ad hoc • Efficiently run on a smartphone without compromising performance, battery life, or reliability

Personalized Contextual Authentication

Mobile Hardware Protection

The Goal: Assurance of Warfighter's Identity, Defense against Compromise

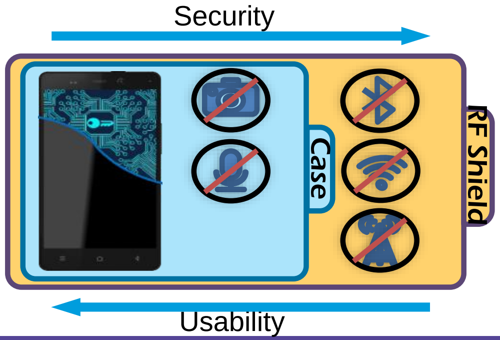
Hardware-Based Protection

- Integration of Mobile device into Secure areas
- 90% of DMUC users use iOS
- Physical and logical sensor blocking and jamming to include RF

Assured Identity Solution

- Leverages off-device CMFA using contextual factors and integrated biometric sensors
- Modular solution to allow increased capabilities in the future

External Modular Security Solution



Virtual Transport Solutions

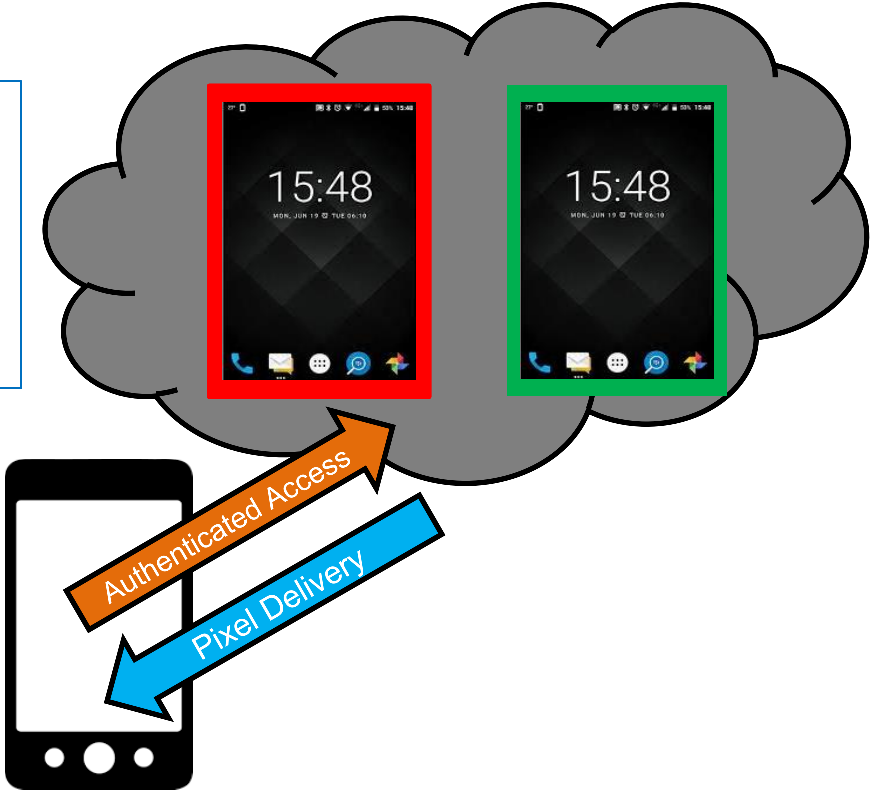
On-Premises Data Security

- Leverage cloud-hosted mobile phone instances to allow multiple classifications on one device
- No data stored on device, allows usage of both Government Furnished Equipment (GFE) and Bring your own (BYOD) devices

Full Device Functionality

- Seamless virtualization on endpoint

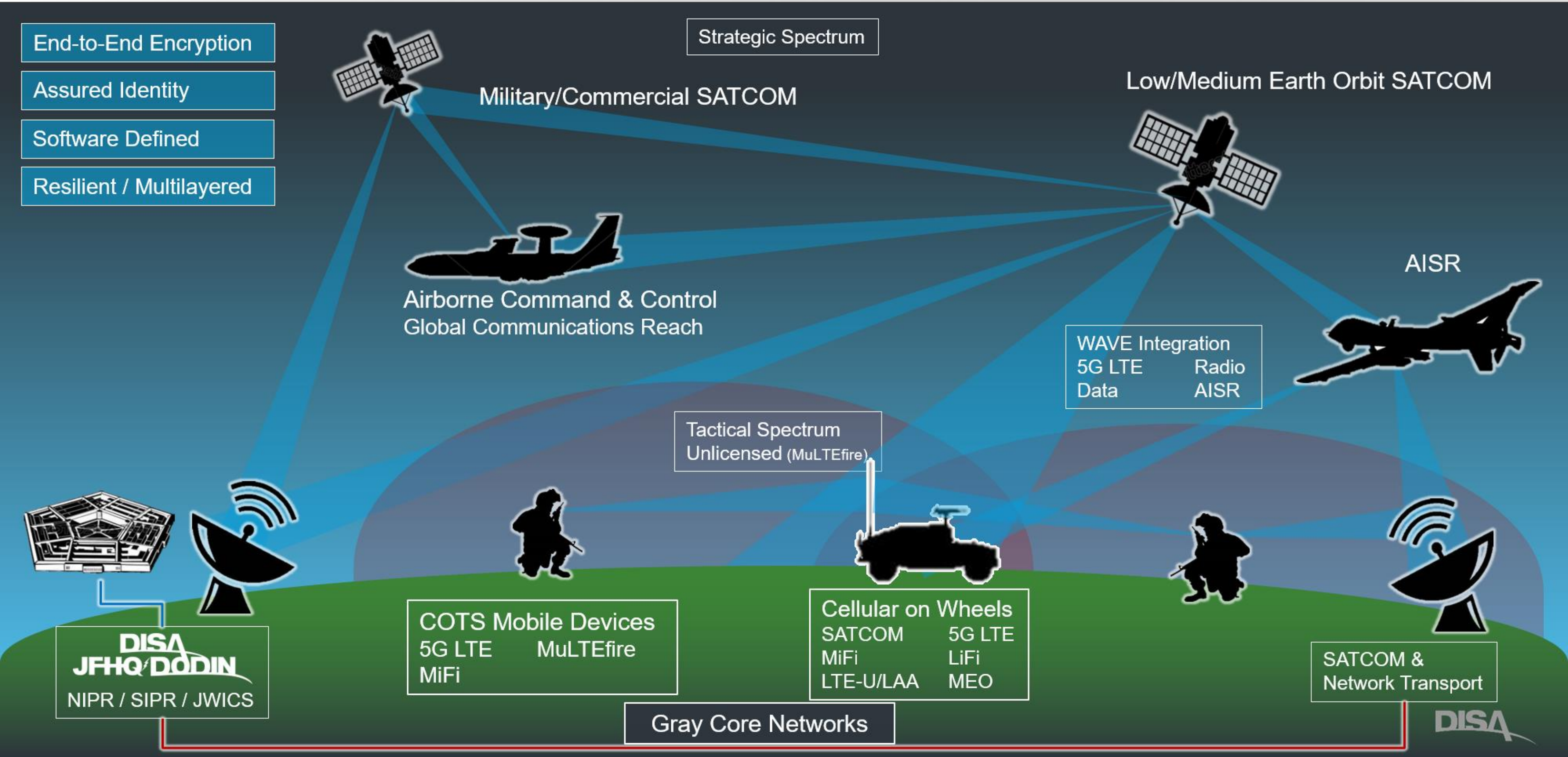
Usage of derived PKI certificates



UNCLASSIFIED

Transport of the Future

From the Foxhole to the Pentagon: Terrestrial – Airborne – Space



End-to-End Encryption

Assured Identity

Software Defined

Resilient / Multilayered

Strategic Spectrum

Military/Commercial SATCOM

Low/Medium Earth Orbit SATCOM

Airborne Command & Control
Global Communications Reach

AISR

WAVE Integration

5G LTE	Radio
Data	AISR

Tactical Spectrum
Unlicensed (MuLTEfire)

DISA
JFHQ DODIN
NIPR / SIPR / JWICS

COTS Mobile Devices

5G LTE	MuLTEfire
MiFi	

Cellular on Wheels

SATCOM	5G LTE
MiFi	LiFi
LTE-U/LAA	MEO

SATCOM &
Network Transport

Gray Core Networks

Machine Learning - Anomaly Detection

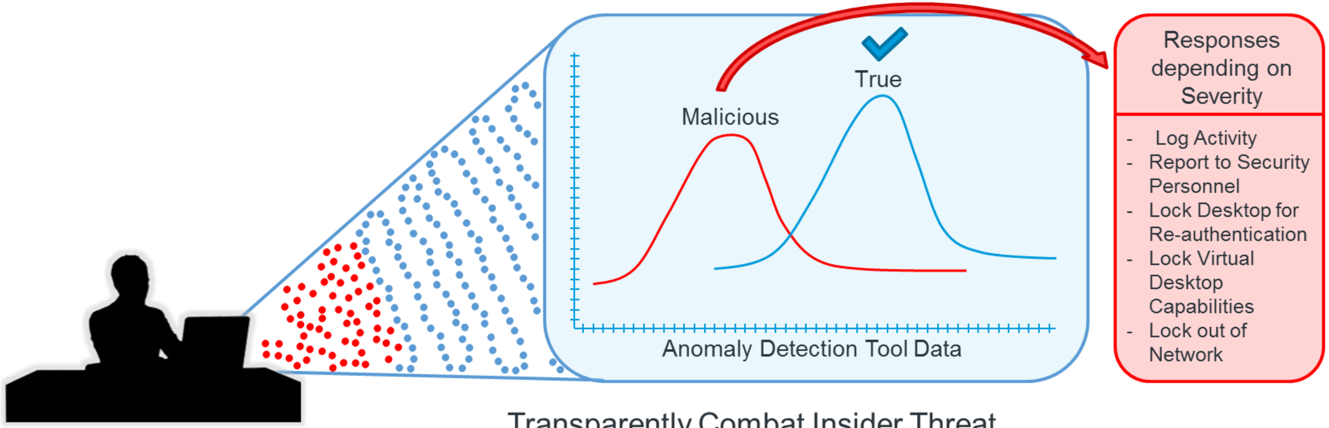
Once given logical access onto workstation, the user’s identity will continue to be validated using:

Machine Learning

Consistently modifies and updates model to more closely identify the user no matter the situation.

Anomaly Detection

Monitors mouse and keyboard interactions and compares them to a known, true model.



Responses depending on Severity

- Log Activity
- Report to Security Personnel
- Lock Desktop for Re-authentication
- Lock Virtual Desktop Capabilities
- Lock out of Network

Transparently Combat Insider Threat

DISA

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**

visit us

DISA Booth 1929

follow us

Facebook/USDISA

Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at **www.disa.mil/about/industry-partners**.